No. 17-2

IN THE

Supreme Court of the United States

UNITED STATES OF AMERICA,

Petitioner,

v.

MICROSOFT CORPORATION,

Respondent.

On Writ of Certiorari to the U.S. Court of Appeals for the Second Circuit

BRIEF OF WASHINGTON LEGAL FOUNDATION AS *AMICUS CURIAE* IN SUPPORT OF RESPONDENT

Richard A. Samp
(Counsel of Record)
Cory L. Andrews
Washington Legal Foundation
2009 Massachusetts Ave., NW
Washington, DC 20036
202-588-0302
rsamp@wlf.org

Date: January 18, 2018

QUESTION PRESENTED

The Stored Communications Act (SCA), 18 U.S.C. § 2701 *et seq.*, imposes restrictions on the dissemination of electronic communications entrusted to email providers but includes a limited exception that permits federal, state, and local governments to demand access to those communications for law-enforcement purposes, pursuant to a warrant.

The question presented is:

Whether invoking the SCA's law-enforcement exception to demand the importation of private electronic communications stored in a foreign country is an impermissible extraterritorial application of the Act.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES v

INTERESTS OF *AMICUS CURIAE* 1

STATEMENT OF THE CASE 2

SUMMARY OF ARGUMENT 6

ARGUMENT 11

I. CONGRESS ADOPTED THE SCA TO ENHANCE PRIVACY OF STORED COMMUNICATIONS, NOT TO INCREASE GOVERNMENT ACCESS TO THEM 11

II. THE PRESUMPTION AGAINST EXTRATERRITORIALITY IS UNREBUTTED AND REQUIRES A FINDING THAT THE SCA DOES NOT AUTHORIZE THE GOVERNMENT TO ACCESS COMMUNICATIONS STORED IN IRELAND 14

A. A Statute's Application Is "Extraterritorial" When, as Here, the Statute Focuses on Subject Matter Associated with Overseas Locations 14

B. The SCA Has a Single Focus; the Section-by-Section Focus Analysis Urged by Petitioner Is Inappropriate 18

Page(s)

C. Petitioner's Section-By-Section Approach to Determining "Focus" Is Unworkable and Leads to Inconsistent Results 21

III. INTERPRETING THE SCA AS AUTHORIZING GOVERNMENTS TO DEMAND PRODUCTION OF COMMUNICATIONS STORED OVERSEAS RAISES SERIOUS FOREIGN POLICY CONCERNS 23

CONCLUSION 25

TABLE OF AUTHORITIES

Page(s)

Cases:

EEOC v. Arabian Am. Oil Co. ["*Aramco*"],
499 U.S. 244 (1991) 1, 7, 18
Foley Bros., Inc. v. Filardo,
336 U.S. 281 (1932) 7
King v. Burwell,
135 S. Ct. 2480 (2015) 20
Kiobel v. Royal Dutch Petroleum Co.,
569 U.S. 108 (2013) 1, 10, 21, 22
Nestle U.S.A., Inc. v. Doe I,
766 F.3d 1033 (9th Cir. 2015),
cert denied, 136 S. Ct. 798 (2016) 22
RJR Nabisco, Inc. v. European Community,
136 S. Ct. 2090 (2016) 1, 9, 14, 19, 21
Microsoft Corp. v. AT&T Corp.,
550 U.S. 437 (2007) 14
Morrison v. Nat'l Australian Bank Ltd.,
561 U.S. 247 (2010) 1, 3, 4, 7, 15, 16, 18,23
Utility Air Regulatory Group v. EPA,
134 S. Ct. 2427 (2014) 20

Statutes:

Alien Tort Statute (ATS),
28 U.S.C. § 1350 ..... 10, 21, 22

Civil Rights Act of 1964, Title VII 16

Electronic Communications Privacy Act (ECPA),
99-508, 100 Stat. 1848 12
Titles I and III,18 U.S.C. §§ 2510-22 12
Title II, 18 U.S.C. §§ 2701 *et seq.* 12

Page(s)

Racketeer Influenced and Corrupt Organizations Act (RICO), 18 U.S.C. §§ 1961-1968 9
18 U.S.C. § 1962 19
18 U.S.C. § 1964(c) 19

Securities Exchange Act of 1934, 15 U.S.C. §§ 78a *et seq.* 9, 16

Stored Communications Act (SCA) 18 U.S.C. §§ 2701 *et seq.* ..... *passim*
18 U.S.C. § 2701 ..... 8, 12, 20
18 U.S.C. § 2702 ..... 8, 12, 20
18 U.S.C. § 2702(b)(8) 24
18 U.S.C. § 2703 ..... 7, 8, 9, 13, 14, 18, 19, 20
18 U.S.C. § 2703(a) & (b) 13

Miscellaneous:

Brief of Ireland as *Amicus Curiae* for Neither Party, *United States v. Microsoft Corp.*, No. 17-2 (Dec. 13, 2017) 24

S. Rep. No. 99-541 (1986) 12

INTERESTS OF *AMICUS CURIAE*

The Washington Legal Foundation (WLF) is a non-profit public interest law firm and policy center with supporters in all 50 states.[1] WLF devotes a substantial portion of its resources to defending free enterprise, individual rights, a limited and accountable government, and the rule of law.

To that end, WLF has regularly appeared before this Court to defend the presumption that, absent clear congressional intent to the contrary, federal legislation does not apply extraterritorially and does not apply to domestic conduct unless that conduct is the "focus" of the legislation. *See, e.g., RJR Nabisco, Inc. v. European Community*, 136 S. Ct. 2090 (2016); *Kiobel v. Royal Dutch Petroleum Co.*, 569 U.S. 108 (2013); *Morrison v. Nat'l Australian Bank Ltd.*, 561 U.S. 247 (2010); *EEOC v. Arabian Am. Oil Co.* ["*Aramco*"], 499 U.S. 244 (1991).

All parties agree that the Stored Communications Act (SCA), 18 U.S.C. § 2701 *et seq.*, includes no language indicating that it applies extraterritorially—and thus it has no such applications. The United States nonetheless argues that its effort to obtain emails stored in Ireland should be deemed a domestic application of the SCA and, accordingly, is sanctioned by the statute.

---

[1] Pursuant to Supreme Court Rule 37.6, WLF states that no counsel for a party authored this brief in whole or in part; and that no person or entity, other than WLF and its counsel, made a monetary contribution intended to fund the preparation or submission of this brief. All parties have consented to the filing; blanket letters of consent have been lodged with the Court.

WLF is concerned that the Government's demand for production of emails stored on servers located overseas is generating diplomatic strife, an issue Congress self-evidently did not address when it adopted the SCA in 1986. More importantly, WLF is concerned that the Government's arguments, if accepted by the Court, would significantly undercut the presumption against extraterritoriality as applied not only to the SCA but also to a wide variety of federal statutes.

WLF recognizes that Congress is empowered to specify that laws it adopts apply outside of our borders. But the decision to apply a statute extraterritorially must be made by Congress, not the courts—no matter how strongly federal officials believe that such application is necessary for law enforcement purposes. The proper response by the Executive Branch to such perceived needs is to propose legislation to Congress that would amend the SCA, not to urge courts to adopt an extraterritoriality analysis that would by-pass Congress's role.

STATEMENT OF THE CASE

As the Second Circuit recognized, the facts of this case are "largely undisputed." Pet. App. 5a. Respondent Microsoft Corp. is an email service provider. It stores its customers' emails on a network of servers located throughout the world. This case involves the efforts of federal prosecutors to obtain access to an unnamed Microsoft customer's emails being stored in Microsoft's datacenter in Ireland (and nowhere else).

In order to maximize its quality of service, Microsoft's policy is to store a customer's emails in the datacenter closest to its customer's residence. Thus, although prosecutors have not publicly revealed the citizenship or residence of their target, there is good reason to believe that he or she does not live in this country but rather lives in or near Ireland.

In 2013, prosecutor invoked the SCA to obtain a warrant from the U.S. District Court for the Southern District of New York, requiring Microsoft to produce all information in its possession associated with the target's email account, including the contents of all emails sent by the target. The court determined that there was probable cause to believe that a crime had been committed and that evidence of the crime could be found in the email account. Microsoft declined to produce emails that it was storing for its customer in Ireland, and it appealed to the Second Circuit from an order holding it in contempt of court for failing to comply with the warrant.

The Second Circuit reversed and remanded to the district court with instructions to quash the warrant. Pet. App. 1a-48a. The appeals court ruled that enforcing the warrant with respect to emails stored in Ireland would constitute an impermissible extraterritorial application of the SCA.

The appeals court explained, "[W]e presume that legislation of Congress 'is meant to apply only within the territorial jurisdiction of the United States,' unless a contrary intent clearly appears." Pet. App. 22a (quoting *Morrison*, 561 U.S. at 255). After determining that the SCA includes no language expressing a

contrary intent of that nature, the court concluded, "Congress did not intend the SCA's warrant requirement to apply extraterritorially." *Id.* at 36a.

The Second Circuit then addressed the second step of *Morrison*'s two-step framework for analyzing extraterritoriality issues: whether Petitioner's requested warrant was merely a domestic application of the SCA. It began its analysis by identifying the "focus" of the relevant SCA provisions: "protecting the privacy of the content of a user's stored electronic communications." Pet. App. 37a. Based on that finding, the court "ha[d] little trouble concluding that execution of the Warrant would constitute an unlawful extraterritorial application of the Act." *Id.* at 43a. It held that "the invasion of the customer's privacy takes place under the SCA where the customer's protected content is accessed"—in this case, Dublin, Ireland. *Id.* at 43a-44a. The court deemed it irrelevant that Microsoft is a U.S. company and that the warrant required disclosure of the stored communications here in the United States (following Microsoft's retrieval of the communications from Ireland). *Id.* at 45a. The court observed that if federal officials seek access to emails stored in a foreign country, they can seek the assistance of the foreign government pursuant to the Mutual Legal Assistance Treaties (MLATs) entered into between the United States and numerous foreign governments (including Ireland). *Id.* at 46a.

Judge Lynch concurred in the judgment. Pet. App. 49a-72a. He recognized that placing emails stored in foreign countries beyond the reach of U.S. court orders might create significant law-enforcement problems. He further recognized that the "balance"

(between privacy concerns and the needs of prosecutors) achieved by barring SCA warrants for emails stored overseas by email service providers "is not likely to constitute the ideal balance of conflicting policy goals." *Id.* at 69a. He nonetheless concluded that because "the decision about whether and when to apply U.S. law to actions occurring abroad is a question that is left entirely to Congress," *id.* at 56a, and because Congress (when it adopted the SCA in 1986) gave no thought whatsoever to extraterritoriality issues, "my colleagues have ultimately reached the right result." *Id.* at 67a.

Judge Lynch concluded that the relief sought by prosecutors should most appropriately be provided by Congress, which "need not make an all-or-nothing choice" of the sort to which the courts are confined. *Id.* at 69a. He explained:

> [Congress] is free to decide, for example, to set different rules for access to communications stored abroad depending on the nationality of the subscriber or of the corporate service provider. It could provide for access to such information only on a more demanding showing than probable cause. ... Or it could adopt other, more creative solutions that go beyond the possibilities evident to federal judges limited by their own experience.

Id. at 69a-70a.

The Second Circuit denied the Government's petition for rehearing *en banc*. Judge Carney wrote an

opinion concurring in the denial, and four judges wrote dissenting opinions. Pet. App. 105a-154a.

SUMMARY OF ARGUMENT

The SCA governs the handling, by email service providers, of emails they are storing on behalf of others. As all parties agree, the Act says absolutely nothing about applying its strictures to communications stored overseas. Under those circumstances, the Second Circuit's conclusion that the Act does not reach communications stored overseas was a straightforward and wholly unobjectionable application of the presumption against extraterritoriality. The appeals court's judgment should be affirmed.

Congress adopted the SCA in 1986, at the infancy of email. It did so because it recognized an emerging threat to privacy. Prior to the 1980s, most written communications were delivered by the U.S. mail or other courier services that maintained control over the paper communications for only a very brief period of time. By contrast, email service providers stored their customers' emails for a far longer period, thereby significantly increasing the chances that the privacy of the author and recipient might be compromised.

The SCA addressed those privacy concerns by making it a criminal offense for anyone to access stored communications without authorization, and by prohibiting email service providers (subject to very limited exceptions) from disclosing stored communications to third parties. One of those

exceptions, set forth in 18 U.S.C. § 2703, authorizes disclosure in response to a warrant obtained by a "government entity" from "a court of competent jurisdiction." Congress included no language in the SCA discussing whether the Act—either its non-disclosure provisions or its limited exceptions—should apply to electronic communications stored overseas.

This Court has repeatedly explained that "legislation of Congress, unless a contrary intent appears, is meant to apply only within the territorial jurisdiction of the United States." *Aramco*, 499 U.S. at 248 (quoting *Foley Bros., Inc. v. Filardo*, 336 U.S. 281, 285 (1932). The presumption against extraterritoriality applies "regardless of whether there is a risk of conflict between the American statute and a foreign law." *Morrison*, 561 U.S. at 255. "When a statute gives no clear indication of an extraterritorial application, it has none." *Ibid.*

The somewhat limited number of emails held by U.S. service providers in 1986 were all being stored on computers maintained in the United States. When adopting the SCA, Congress did not contemplate (and could not have contemplated) the possibility that stored communications might travel instantaneously across international borders. Accordingly, the SCA did not address: (1) protecting privacy with respect to emails stored abroad; and (2) creating a warrant exception to allow for limited disclosure of emails stored abroad. Given that omission, *Morrison* dictates that the SCA has no application to electronic communications stored abroad.

There is no merit to Petitioner's argument that

its effort to enforce a warrant for communications stored in Ireland is nothing more than a domestic application of the SCA. Petitioner points out that Microsoft has a principal place of business in this country. It asserts that invocation of § 2703's warrant procedures is consistent with common-law subpoena procedures that (according to Petitioner) would have allowed federal and state governments to demand that a U.S. company produce all documents within its control—even documents stored overseas. But even if that assertion were correct (and WLF disputes that assertion with respect to overseas documents belonging to a third party), it does not support Petitioner's claim that its warrant constitutes a domestic application of the SCA. The Second Circuit correctly determined that protecting the privacy of "stored communications" is the "focus" of the SCA. Because the stored communications constituting the "focus" of this dispute are located overseas, Petitioner's efforts to obtain those communications cannot plausibly be characterized as a domestic application of the SCA.

Petitioner contends that the "focus" of § 2703 is different from the focus of §§ 2701 and 2702 (which bar unauthorized third-party access to stored communications and impose strict limits on the authority of email service providers to disclose those communications). Petitioner contends that the "focus" of § 2703 (which contains the SCA's warrant provisions) is disclosure of stored communications. Because its warrant requires Microsoft to disclose the contested emails to prosecutors here in the United States, Petitioner argues that its warrant simply seeks to apply the SCA in a domestic context.

WLF agrees with Microsoft that even if § 2703 were examined in isolation, its "focus" would be protecting the privacy of the owners of stored communications—in particular, the limited circumstances under which those privacy interests may be overcome. But more importantly, Petitioner's section-by-section approach to determining statutory "focus" is unsound and has never been endorsed by this Court. Petitioner cites *RJR Nabisco* in support of its section-by-section approach, but that case never even reached the "focus" issue (step two of the traditional approach to adjudicating extraterritoriality questions). Rather, the Court confined its analysis to determining whether Congress intended extraterritorial application of the liability and cause-of-action provisions of the Racketeer Influenced and Corrupt Organizations Act (RICO), 18 U.S.C. §§ 1961-1968. *RJR Nabisco*, 136 S. Ct. at 2101-2111. In its opinion setting forth its most detailed explanation of the "focus" inquiry (*Morrison*), the Court discerned but a single "focus" of the relevant provisions of the Securities Exchange Act of 1934, 15 U.S.C. §§ 78a *et seq.*, and never suggested that a separate "focus" inquiry should be undertaken for every section of interconnected statutory provisions.

A fundamental objection to Petitioner's section-by-section approach is that it deprives the "focus" inquiry of clarity, thereby making it exceedingly difficult for lower courts to apply it in a uniform manner. While all can agree, for example, that the overriding purpose of the SCA is to protect the privacy of stored information, there are no clear guideposts for determining whether the "focus" of § 2703 (when viewed in isolation) should be viewed as a strictly limited exception to the SCA's privacy provisions or (as

Petitioner suggests) a free-standing grant of government entitlement to disclosure of stored communications.

A perceived lack of clarity in the step-two "focus" analysis has led to conflicting appeals court decisions addressing extraterritoriality issues arising under the Alien Tort Statute (ATS), 28 U.S.C. § 1350. The Court determined in *Kiobel* that Congress did *not* intend the ATS (which creates federal court jurisdiction for a small number of claims by aliens alleging violations of the law of nations) to apply extraterritorially. *Kiobel*, 569 U.S. at 124. Because most ATS claims pending in federal courts assert that a U.S.-based company aided and abetted human rights violations committed overseas by others (often, a foreign government), one might have supposed that those claims would be dismissed in light of *Kiobel*—after all, the circumstances that are the plain focus of the ATS (violations of the law of nations) all occurred overseas. However, federal appeals courts have adopted conflicting interpretations of the "focus" test, with the result that several courts have declined to dismiss ATS claims that allege overseas human rights violations by U.S.-based companies. WLF urges the Court to eliminate this confusion by clarifying that a set of interlocking statutory provisions should be deemed to have but a single "focus" for purposes of determining whether they are being applied domestically or extraterritorially.

Petitioner's approach should also be rejected because it would create a host of practical problems. Most prominently, it is likely to create friction with

foreign governments, and indeed (as evidenced by various *amicus curiae* briefs filed in this case) it already has. Under Petitioner's approach, any government—federal, state, or local—would be permitted to demand that a foreign corporation conducting business in this country produce communications stored anywhere in the world, even if the emails in questions have no connection with the United States. WLF respectfully submits that Congress, not a court, is the body that most appropriately determines whether law-enforcement considerations outweigh the foreign-relations costs likely to be incurred as a result of such demands.

ARGUMENT

I. CONGRESS ADOPTED THE SCA TO ENHANCE PRIVACY OF STORED COMMUNICATIONS, NOT TO INCREASE GOVERNMENT ACCESS TO THEM

Petitioner's citation to the SCA as the basis for its claimed right to require disclosure of electronic communications stored in Ireland is ironic. Both the text of the statute and its legislative history demonstrate that Congress adopted the SCA to protect the privacy of communications being stored by email service providers, not to increase the authority of governments to pry into private communications.

What we now refer to as email began to develop in the early 1980s. Advances in technology permitted individuals to transmit written communications electronically—and they could do so much more quickly via electronic means than by using the U.S. Mail or

other courier services. Congress adopted the SCA in response to concerns that growth of electronic communications would be impeded unless the privacy of communications sent via email could be assured. Lack of privacy protections was of particular concern because, as Congress recognized, email service required that electronic communications be stored on the computers of email service providers for lengthy time periods. S. Rep. No. 99-541, at 3-5 (1986).

The privacy focus of the SCA is demonstrated by the title of the legislation of which it formed a part: the Electronic Communications Privacy Act, Pub. L. 99-508, 100 Stat. 1848 (1986).[2] As the Second Circuit explained, the SCA was designed to "protect[ ] the privacy of the contents of files stored by service providers and of records held about the subscriber by service providers, according to the Justice Department." Pet. App. 13a.

The initial section of the SCA, 18 U.S.C. § 2701, prohibits unauthorized third parties from, *inter alia*, obtaining access to electronic communications stored by a service provider. Section 2702 impose strict limits on the authority of service providers to disclose those communications, subject to several exceptions—including disclosures made in response to an authorized government demand. Section 2703 sets

---

[2] The SCA is Title II of the ECPA. Title I prohibits the interception of wire, oral, or electronic transmissions. Title III requires government entities to obtain court orders before installing pen registers or trap and trace devices. *See* 18 U.S.C. §§ 2510-22.

forth the conditions under which a government is authorized to obtain access to stored electronic communications. In order to obtain access to recently stored communications, or to obtain access to older communications without first notifying the customer, the government must obtain "a warrant, issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, using State warrant procedures) by a court of competent jurisdiction." 18 U.S.C. §§ 2703(a) & (b).

There is no hint in either the text or legislative history of the SCA that Congress adopted § 2703 for the purpose of expanding government access to stored electronic communications. Rather, all available evidence indicates that the SCA was designed to strengthen the privacy rights of the authors and recipients of emails and that Congress included § 2703 for the purpose of creating limited exceptions to the Act's privacy provisions—by describing limited circumstances under which governments would be permitted to gain access to stored communications.

More importantly for purposes of this case, the SCA includes no language suggesting that the Act (including the provisions of § 2703) applies to electronic communications stored outside of the United States. Indeed, the parties are in complete agreement that Congress in 1986 did not contemplate that U.S. email service providers might store electronic communications overseas—and that, accordingly, it had had no occasion to address the issue.

II. THE PRESUMPTION AGAINST EXTRATERRITORIALITY IS UNREBUTTED AND REQUIRES A FINDING THAT THE SCA DOES NOT AUTHORIZE THE GOVERNMENT TO ACCESS COMMUNICATIONS STORED IN IRELAND

The well-accepted presumption against extraterritoriality has been explained by the Court as follows: "Absent clearly expressed congressional intent to the contrary, federal laws will be construed to have only domestic application." *RJR Nabisco*, 136 S. Ct. at 2100. The presumption is an outgrowth of "a basic premise of our legal system that, in general, 'United States law governs domestically but does not govern the world.'" *Ibid* (quoting *Microsoft Corp. v. AT&T Corp.*, 550 U.S. 437, 454 (2007)).

As noted above, Petitioner does not contest the absence of any "clearly expressed congressional intent" that the SCA should govern the world and concedes that the SCA is inapplicable outside the United States. It nonetheless argues that it is entitled to invoke § 2703 to demand access to electronic communications stored in Ireland, insisting that its demand constitutes a mere domestic application of the SCA. That counter-intuitive assertion finds no support in this Court's case law.

A. A Statute's Application is "Extraterritorial" When, as Here, the Statute Focuses on Subject Matter Associated with Overseas Locations

A finding that Congress did not intend

extraterritorial application of a statute does not necessarily resolve an extraterritoriality dispute. When a party contends that its attempted invocation of a statute is merely domestic in character, courts turn to "step two" of the traditional approach to adjudicating extraterritoriality questions—a process that requires identifying the "focus" of the statute in question.

Once a statute's "focus" (or "the object[ ] of the statute's solicitude") is identified, courts should apply that focus to determine whether a party's proposed application of the statute should be deemed extraterritorial; the application is extraterritorial when the subject matter upon which the statute principally focuses is associated with overseas locations. *Morrison*, 561 U.S. at 266-67. *Morrison* stated that the proposed application cannot escape being classified as "extraterritorial" simply because it has *some* connection with the United State:

> [I]t is a rare case of prohibited extraterritorial application that lacks *all* contact with the territory of the United States. But the presumption against extraterritorial application would be a craven watchdog indeed if it retreated to its kennel whenever *some* domestic activity is involved in the case.

Id. at 266 (emphasis in original). *Morrison* pointed to *Aramco* as an example of that principle. *Aramco* held that a suit alleging that an American company engaged in invidious employment discrimination against employees working in Saudi Arabia sought an

improper extraterritorial application of Title VII of the Civil Rights Act of 1964—notwithstanding the fact that the employee had been hired in Houston and was an American citizen. *Morrison*, 561 U.S. at 266. Although some portions of the employment relationship were associated with the United States, the focus of Title VII is the prevention of employment discrimination, and the allegedly discriminatory acts occurred overseas.

Morrison employed its "focus" analysis to conclude that litigants alleging securities fraud in violation of the Securities Exchange Act were seeking an improper extraterritorial application of the Act. Based on its examination of a number of provisions in the Exchange Act (including its prologue), the Court concluded that the Act's "focus" is purchases and sales of securities in the United States. *Ibid.* The plaintiffs alleged that the defendants engaged in extensive fraud within the United States, but their damage claims rested on an allegation that the U.S.-based fraud affected the purchase and sales of securities that occurred in Australia. Because the purchases and sales lacked any significant U.S. connection, the Court concluded that the Exchange Act had no application to those transactions. *Id.* at 266-67.

An analysis of the SCA's focus—the protection of stored communications from unauthorized disclosures, in order to protect the privacy interests of the customers of email service providers—leads to a similar result. The location most closely associate with that statutory focus is the place where the targeted emails were stored by Microsoft—in this case, Dublin, Ireland. Because that location is overseas, the SCA (a

statute that does not apply extraterritorially) is inapplicable to this case. The customer (as well as Microsoft) must look to Irish law to protect the privacy of the stored electronic communications; and federal, state, and local governments must look to Irish law as well if they wish to demand access.

The only other location plausibly associated with the "focus" of the SCA is the country of residence/citizenship of the owner of the emails. Given Microsoft's policy of storing emails at the datacenter closest to what it believes to be the customer's place of residence, the targeted customer most likely lives in or near Ireland and almost certainly does not live in the United States.[3] In any event, Petitioner has not submitted evidence that the target is, in fact, a citizen or resident of the United States. So Petitioner's proposed application of the SCA should be deemed extraterritorial even if the Court were to conclude that the SCA's "focus" is most closely associated with the residence/citizenship of the email owner whose privacy is being protected.

---

[3] Indeed, because Petitioner plainly knows the place of residence of the individual it is targeting, one can reasonably expect that it would have disclosed that residence to the Court were the target a U.S. resident. Thus, its failure to disclose residence is a strong indication that the target neither resides in this country nor is a U.S. citizen.

B. The SCA Has a Single Focus; the Section-by-Section Focus Analysis Urged by Petitioner Is Inappropriate

This matter's single domestic connection is Microsoft's residence: it is incorporated in the United States and maintains its principal place of business here. But as *Aramco* and *Morrison* make clear, the presumption against extraterritoriality cannot be overcome simply by demonstrating that "*some* domestic activity is involved in the case." *Morrison*, 561 U.S. at 266.

Petitioner does not contest that the "the object of the [SCA's] solicitude," *id.* at 267, is protecting the privacy of electronic communications being stored by email service providers. Petitioner nonetheless contends that the Court's "focus" analysis requires that every section of the SCA be addressed separately—and that it should be deemed to be applying the Act domestically if the precise statutory provision it seeks to invoke has a "focus" associated with a location in the United States. It further contends that the "focus" of § 2703 is the disclosure of electronic communications under Microsoft's control and that Microsoft (as a corporation with a U.S. presence) can be compelled to transfer stored communications from Ireland to the U.S. and then produce them domestically.

WLF agrees with Microsoft that even if the "focus" of § 2703 were considered in isolation, Petitioner's efforts to invoke that provision in this case would constitute an extraterritorial application of the

SCA. As fully explained by Microsoft and the Second Circuit, Section 2703's imposition of a "warrant" requirement is a strong textual indication that Congress did not intend to permit federal, state, and local government officials to demand access to communications stored overseas.

More importantly, Petitioner's section-by-section approach to determining statutory "focus" is unsound and has never been endorsed by this Court. Petitioner cites *RJR Nabisco* in support of its section-by-section approach, but that case never even reached the "focus" issue (step two of the traditional approach to adjudicating extraterritoriality questions). Rather, the Court confined its analysis to determining whether Congress intended extraterritorial application of the liability and cause-of-action provisions of RICO. *RJR Nabisco*, 136 S. Ct. at 2101-2111.

The Court's separate consideration of Congress's intent with respect to RICO's liability provisions, 18 U.S.C. § 1962, and its civil-cause-of-action provision, 18 U.S.C. § 1964(c), was fully consistent with its longstanding approach to applying the presumption against extraterritoriality. The Court recognized that Congress might plausibly have intended some of RICO's prohibitions to apply to conduct occurring outside the United States while simultaneously denying a right of action to individuals injured by such conduct—because "providing a private civil remedy for foreign conduct creates a potential for international friction beyond that presented by merely applying U.S. substantive law to that foreign conduct." *Id.* at 2106. Separate consideration of the two provision was

mandated by the presumption against extraterritoriality, the Court explained, because "when a statute provides for some extraterritorial application, the presumption against extraterritoriality operates to limit that provision to its terms." *Id.* at 2102. But contrary to Petitioner's contention, *RJR Nabisco* never suggested that RICO should be deemed to have more than one "focus" for purposes of determining whether the plaintiffs were proposing domestic application of the statute.

Petitioner's efforts to consider § 2703 in isolation cuts against well-established canons of statutory construction. This Court has explained that a court's "duty" is "to construe entire statutes, not isolated provisions." *King v. Burwell*, 135 S. Ct. 2480, 2489 (2015). It is a "fundamental canon of statutory construction that the words of a statute must be read in their context and with a view to their place in the overall statutory scheme." *Utility Air Regulatory Group v. EPA*, 134 S. Ct. 2427 (2014). When read in the context of the entire SCA, § 2703 quite plainly is a closely interlocking part of an overall statutory scheme designed to protect the privacy of stored communications while recognizing limited exceptions to that privacy—not a free-standing grant of authority to federal, state, and local officials to demand access to private communications. To cite just one of the many textual clues: § 2703 is expressly cited in both § 2701 and § 2702 as an "exception" to the broad privacy protections afforded by those two sections to stored communications. And, of course, nothing within the statutory "exception" provides any indication that Congress intended it to have extraterritorial effect.

C. Petitioner's Section-By-Section Approach to Determining "Focus" Is Unworkable and Leads to Inconsistent Results

Petitioner's section-by-section approach to determining "focus" should also be rejected because it is unworkable. As *RJR Nabisco* noted, "It is a rare case of prohibited extraterritorial application that lacks *all* contact with the territory of the United States." *RJR Nabisco*, 561 U.S. at 266. If courts must examine every section of a statute already determined to have no extraterritorial application—in order to determine whether at least one of the sections "focuses" on a subject matter that is associated with a domestic location—the extraterritoriality analysis will become extremely cumbersome. And because the party seeking to invoke the statute will almost always be able to point to *some* contact with the United States and to plausibly argue that that contact bears some relationship to the focus of at least one section of the statute, inconsistent judicial decisions are inevitable.

The post-*Kiobel* history of ATS litigation starkly illustrates the need for a clear and easily applied "focus" test. The Court determined in *Kiobel* that Congress did *not* intend the ATS (which creates federal court jurisdiction for a small number of claims by aliens alleging violations of "the law of nations") to apply extraterritorially. *Kiobel*, 569 U.S. at 124. Because most ATS claims pending in federal courts assert that a U.S.-based company aided and abetted human rights violations committed overseas by others (often, a foreign government), one might have supposed

that those claims would be dismissed in light of *Kiobel*—after all, the circumstances that are the plain focus of the ATS (violations of the law of nations) all occurred overseas.

But numerous ATS claims based on alleged overseas human rights violations continue to thrive in the lower courts, in large measure due to confusion regarding how to apply the step-two "focus" test to these claims. The Ninth Circuit, for example, has concluded that ATS claims are being applied domestically if a U.S.-based corporate defendant takes at least some actions within the United States that bear some relationship to human rights violations that occur overseas. *Nestle U.S.A., Inc. v. Doe I*, 766 F.3d 1033 (9th Cir. 2015), *cert. denied*, 136 S. Ct. 798 (2016). Indeed, the Ninth Circuit even questioned whether the step-two "focus" test has any application in the context of claims arising under the ATS. *Id.* at 1018.

The Court can eliminate much of the current confusion regarding the "focus" test by mandating that once a court determines that a statute consisting of interlocking provisions has no extraterritorial applications, it should identify the *single*, dominant focus of those provisions for purposes of ascertaining whether the court is being asked to apply the statute domestically or extraterritorially.

III. INTERPRETING THE SCA AS AUTHORIZING GOVERNMENTS TO DEMAND PRODUCTION OF COMMUNICATIONS STORED OVERSEAS RAISES SERIOUS FOREIGN POLICY CONCERNS

Petitioner's proposed construction of the SCA should also be rejected because it would create a host of practical problems. Most prominently, it is likely to create friction with foreign governments, and indeed (as evidenced by various *amicus curiae* briefs filed in this case) it already has.[4] Under Petitioner's approach, any government—federal, state, or local—would be permitted to demand that a foreign corporation conducting business in this country produce communications stored anywhere in the world, even if the emails in questions have no connection with the United States. It is unlikely that Congress ever intended to grant local officials unilateral authority to act in a manner that could place the United States into conflict with its allies.

Moreover, the United States has available to it alternative means to obtain the stored communications it seeks. Ireland's *amicus* brief indicates that it would expeditiously consider any request from U.S. government officials for access to electronic

---

[4] The Court has determined, moreover, that the presumption against extraterritoriality exists in large measure because of the ever-present *potential* for friction with foreign governments. It applies without regard to whether any friction is likely to develop. *Morrison*, 561 U.S. 2877-78 ("The canon or presumption applies regardless of whether there is a risk of conflict between the American statute and a foreign law.").

communications stored in Ireland:

> Ireland continues to facilitate cooperation with other states, including the United States, in the fight against crime. Indeed, Ireland and the United States are already parties to a treaty [the MLAT] addressing the subject of this appeal. ... Ireland therefor considers that the procedures provided for in the MLAT represent *the most appropriate means* to address requests such as those which are the object of the warrant in question.

Brief for Ireland as *Amicus Curiae* in Support of Neither Party (Dec. 13, 2017) at 2 (emphasis added).[5]

WLF does not contest that the decision below may be causing some difficulties for law-enforcement officials—at least in non-emergency situations. *See* 18 U.S.C. § 2702(b)(8) (authorizing email service providers to unilaterally decide to release emails to a "government entity" in "an emergency involving danger of death or serious physical injury"). Properly balancing privacy concerns, foreign policy concerns, and law-enforcement needs can be a very difficult proposition. But as Judge Lynch stated in his concurring opinion, because "the decision about whether and when to apply U.S. law to actions

---

[5] Petitioner asserts that in other cases it may be difficult to determine precisely where electronic communications are stored. In *this* case, however, the precise location where the communications are stored (Ireland) is uncontested.

occurring abroad is a question that is left entirely to Congress," Pet. App. 56a, and because Congress (when it adopted the SCA in 1986) gave no thought whatsoever to extraterritoriality issues, the proper course for the courts is to stay their hands while Congress determines how best to update the SCA. *Id.* at 67a-70a.

WLF respectfully submits that Congress, not a court, is the body that most appropriately determines whether law-enforcement considerations outweigh the foreign-relations costs likely to be incurred as a result of demands for electronic communications stored overseas.

CONCLUSION

The decision below should be affirmed.

Respectfully submitted,

Richard A. Samp
(Counsel of Record)
Cory L. Andrews
Washington Legal Found.
2009 Massachusetts Ave., NW
Washington, DC 20036
202-588-0302
rsamp@wlf.org

January 18, 2018